2023

A Scoping Review of Hacking Back in Cybersecurity

Calvin Nobles

A Scoping Review of Hacking Back in Cybersecurity

Calvin Nobles
Illinois Institute of Technology
cnobles1@iit.edu

ABSTRACT

Hacking back or retaliating against cyber attackers through offensive means is a controversial and complex issue that has garnered significant attention recently. This paper provides a valuable resource for understanding the complexities and implications of hacking back in the context of cybersecurity. This paper provides a scoping review of the existing literature on hacking back, focusing on a standardized definition, identifying trends in the literature, and exploring alternatives to counterattacking. Based on the analysis, the study finds that hacking back is a subject with polarizing viewpoints on its effectiveness and ethics. While some argue that it is a necessary tool to deter cyber attackers and protect against threats, others raise concerns about its legality and potential unintended consequences. The study highlights the need for further empirical and scholarly research to explore alternative solutions, attribution, legal frameworks, and modifications to existing laws on hacking back.

Keywords

Active Cyber Defense, Attribution, Counter-hacking, Cyber-attacks, Cybersecurity, Hacking Back

INTRODUCTION

U.S. corporations face continuous cyber-attacks with severe consequences but cannot hack back beyond their digital infrastructure (Holzer & Lerums, 2016). The recurring debate on hacking back is due to US commissions and think tanks exploring the issue (Broeders, 2021). Inaction or prohibiting retaliation is futile and encourages more attacks by malicious actors (Rabkin & Rabkin, 2016). However, the topic of retaliatory action in response to cyber-attacks remains unresolved, particularly as companies become more capable of carrying out offensive cyber operations.

Opposition to hacking back is vital due to concerns of conflict escalation and empowering private entities to engage with illicit actors (Fisher, 2013). Cyber experts argue that such actions should be left to the government (Rundle, 2021). Moreover, corporations have limited options beyond cybersecurity defense to protect against persistent hackers (Fiotakis), 2021) as malicious cyber activity has expanded beyond physical boundaries (Change & Whitehead, 2022). However, there is a lack of empirical research on hacking back, leaving stakeholders without a holistic understanding of the issue (Housen-Couriel, 2021).

Hacking back, or the active defense against cyberattacks by retaliating against the perpetrators has gained traction in recent years as organizations and governments face increasingly sophisticated threats (Broeders, 2021; Holzer & Lerums, 2016). However, this approach raises significant ethical, legal, and technical concerns that must be addressed. The primary challenge is to develop a comprehensive framework for hacking back that balances the need for robust cybersecurity measures with the potential risks associated with aggressive countermeasures while also adhering to national and international legal norms.

In this paper, I utilized a scoping review, a relatively new approach to evidence synthesis through a comprehensive and structured literature search (Levac et al., 2010). This scoping review aims to identify a standardized definition of hacking back, alternatives to hacking backing, literature trends, and future research direction.

HACKING BACK

Hacking back involves identifying hackers and counterattacking the identified perpetrators (Holzer & Lerums, 2016; Thomas, 2017). However, the concept is controversial, with concerns about criminality and the potential for cyberwarfare (Couzigou, 2020; Smith, 2017). Hacking back is prohibited under the Computer Fraud and Abuse Act, but proposed legislation, such as the Active Cyber Defense Certainty Act, aims to empower organizations to protect themselves (Porch, 2020). While still controversial, such proposals highlight an assertive approach to combating cyber-attacks. Companies use passive defensive measures such as honey pots to gain insights into intruder tactics, techniques, and procedures. A honeypot is an entity whose value and benefits are derived from being attacked or compromised (Guo et al., 2022). This suggests that a honeypot is an intentionally created system, expected to be scrutinized and potentially exploited. Instead of repairing or retaliating, a honeypot

is an authentic, high-value data storage mechanism (Guo et al., 2022). Honeypots supply additional, essential information about the characteristics of cyberattacks.

RESEARCH METHOD

A scoping review aims to encompass a broader range of literature and address more general questions (Arksey & O'Malley, 2005; Kavanaugh et al., 2016). Munn et al. (2018) stated that scoping reviews help investigate the scope, breadth, and characteristics of research endeavors in a developing field and pinpoint gaps in the current literature. Utilizing a scoping review as a systematic approach is suitable for exploring the current trends and state of knowledge and identifying alternatives to hacking back and crucial research paths for future investigations.

SEARCH STRATEGY

The scoping review process comprises five sequential steps: (a) defining the research topic, (b) identifying pertinent studies, (c) choosing relevant studies, (d) gathering data and assembling, condensing, and (e) presenting findings. Table 1 illustrates the methodology utilized to collect evidence for this review. The search was narrowed down to hacking back, striking back, and hack backs in the cybersecurity field in the United States, with all types of publications, articles, and proceedings included. The scoping review encompassed the timeframe from January 2002 to February 2023.

Inclusion Criteria	Exclusion Criteria
• Peer-reviewed papers on hacking back or striking back in cybersecurity • Peer-reviewed book chapters • English language only • Periodicity: 2000-2023	• Nonpeer-reviewed papers • Books • Hacking or striking back does not mean taking retaliatory action

Table 1: Inclusion and Exclusion Criteria

I used several databases, including Scopus, IEEE, and ACM, for this scoping review. The primary objective of employing these databases was to optimize the search for peer-reviewed articles on hacking or striking back in cybersecurity. Most of the peer-reviewed content in Scopus, the largest repository, is in English (Adam et al., 2019). The three databases mentioned above were used to identify published studies. These databases are often deemed more comprehensive than others because they include research papers on a broad spectrum of cybersecurity and technology topics. Scopus was chosen since it enables the search for articles using predefined keywords, such as those in the title, abstract, or keywords. According to Abbas et al. (2021, 2022) and Ali et al. (2021), Scopus is one of the most exhaustive databases of abstracts and citations for peer-reviewed literature. At this stage, the sample size was 464 articles, which were later excluded from the final round because they did not pertain to hacking or striking back. Figure 1 depicts the search strategy and criteria.

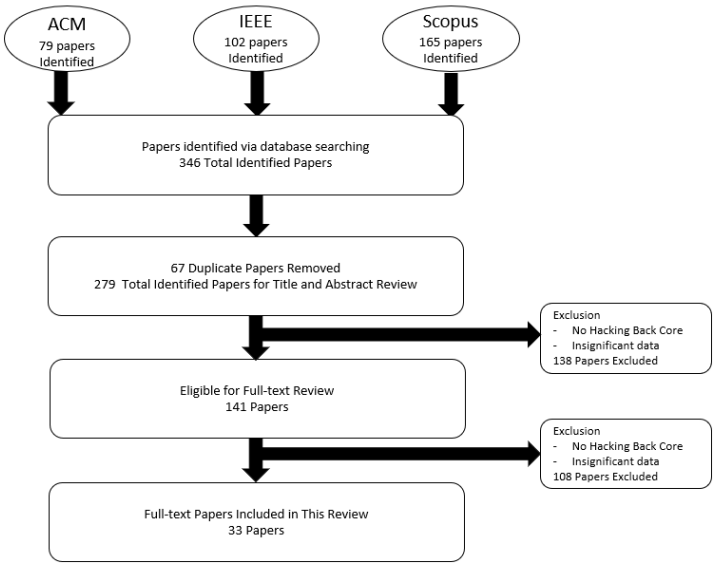

Figure 1. Process for Article Identification and Selection

RESULTS, ANALYSIS, AND FINDINGS

Hacking Back Definitions	
Definitions	**Reference(s)**
A hack back refers to any action taken with the intention of: (a) Launching a counterattack in response to a cyber-attack, regardless of who is the attacker (b) Retrieving or reclaiming stolen artifacts such as exfiltrated data, documents, or cryptocurrency (c) Disrupting the computing infrastructure utilized by the attackers to carry out their hacking. (d) Identifying the attacker(s) and reporting them to law enforcement agencies .	Badhwar & Badhwar (2021)
Hacking back refers to the proactive measures taken by a victim of a cyberattack to retaliate against their assailant. The terms hacking back, retaliatory hacking, and counter hacking are used interchangeably.	Gallagher (2022); Boussios (2021); Holzer & Lerums (2016); Iasiello (2014)
Hacking back is the victim's retaliation against the attacker following a cyber-attack. This type of hacking is not an unprovoked first strike but rather a response to an attack.	Martens & Cuijpers (2021)
Hacking-back encompasses a wide range of offensive cyber tactics aimed at attacking attackers. One such tactic involves security professionals setting up a series of automatic or manually triggered responses called active defenses.	Gross (2015); Couzigou (2020); Cook (2018); Balitzer (2015)
Hacking back is classified as an active cyber defense to engage the attacker using counter-hacking methodologies that are destructive and damaging.	Iasiello (2014)

Table 2: Definitions of Hacking Back

While all the articles mentioned hacking back, most did not define hacking back. Martens and Cuijpers (2021) indicated that hacking back is not well defined; from the Table above, the definitions are centric on retaliating against initial cyber attackers using active cyber defense methodologies. The definition is not completely standardized, but most examined definitions of hacking back are closely related.

Alternatives to Hacking Back	
Alternatives to Hacking	**Reference(s)**
A major part of this proposed strategy would be using a team of government technicians to find these attackers and execute a counterattack called a "hack-back	Welker & Abiona (2021)
One alternative solution is establishing a government subsidy to implement and enhance safeguards on networks based in the US. A significant component of this alternative approach involves employing a team of government technicians to identify attackers and conduct retaliatory strikes.	Welker & Abiona (2021)
An ideal alternative is aggressive cyber defense, a proactive security measure.	Iasiello (2014)
Ethical hacking. Leave hacking back to the government.	Formosa et al. (2021); Rundle (2021)
The US government already utilizes a form of "name and shame" by threatening or implementing commercial sanctions on foreign companies that compete with US firms or gain from US intellectual property theft if hackers are linked to them—the do-nothing approach.	Rabkin & Rabkin (2016)

Table 3: Alternatives to Hacking Back

Table 3 reflects the alternatives to hacking back. The explored literature provided the capture alternatives to hacking back based on the concerns of counterattacking (listed in Table 4 under Rationale Against Hacking Back). The alternatives to hacking back primarily consist of strategies to prevent organizations from escalating and breaking laws.

Trends in Literature	
Rationale Against Hacking Back:	**Reference(s)**
The no-to-private hack back camp argues that the risk of an escalating retaliatory counterattack makes hacking back a losing proposition. This is because not all private actors possess the same level of knowledge and expertise regarding hacking. Counterattacks are ineffective.	Badhwar & Badhwar (2021); Brunoni (2016); Kallberg, 2015; Ryan (2018)
It is important to note that hacking back a hacker or hacking syndicate can trigger a counterattack, resulting in cyber warfare that may cause even more destruction and harm to the economies of affected businesses or countries.	Badhwar & Badhwar (2021)
Non-State actors engaging in hacking-back activities violate national legal systems and contravene the principles of the rule of law at the municipal level.	Christen (2020); Cook (2018); Couzigou (2020)
The idea of hacking back poses several problems. Attribution difficulties make it risky, exposing organizations to liability. The aggressor may evade retaliation, incentivizing continued attacks. Private actors often do not have the advanced tools and information for attribution that the government has, making them susceptible to mistakenly hacking back against innocent parties.	Lemay & Leblanc (2021); Iasiello (2014); Holzer & Lerums (2016)
The attribution debate is progressing sluggishly and primarily concentrated on technical forensics; however, attribution remains challenging and demands significant time, specialized abilities, and the potential for a skilled adversary to obscure its tracks through routing attacks or exploitations via anonymous global computers.	Withers et al., (2020)
Rationale for Hacking Back:	
Non-State actors argue they should be allowed to hack back because States cannot effectively protect them from harmful cyber operations. Private actors may be more capable than States regarding attributing and responding to cyber-attacks. The Commission on the Theft of American Intellectual Property says that US companies should hack back at cyber-thieves.	Couzigou (2020); Fernandes et al (2014)
The legality of hacking back is dubious, as it may be considered a form of "self-defense" that could potentially justify offensive actions on moral grounds. An option could be for the employer to act on behalf of the company and disrupt the operations of a foreign business engaged in industrial espionage.	Christen et al (2017)
Policymakers worldwide support greater autonomy for companies to defend against cyber attackers. Lawmakers and scholars have proposed amending the CFAA to enable private parties to obtain information from and damage the systems of hackers since critics argue that the CFAA could restrict private parties' ability to "hack back" against attackers, which could impede their capacity to prevent and mitigate cyber-attacks.	Kosseff (2017); Shackelford et al. (2019)
Although hard law on cybersecurity exists in the US and internationally, it was created when proactive cybersecurity was still in its infancy, thus prompting the private sector to spearhead industry norm development.	Craig et al. (2015)
Corporations Fighting Back	
U.S. corporations are already hacking back. Company officials are now ready to hack back to uncover hackers and eradicate stolen data, a notion previously deemed too dangerous to propose.	Messerschmidt (2013); Brunoni (2016); Holzer & Lerums (2016)
While Google's admission of "hack back" was noteworthy, private companies, including those on the Fortune 500 list, are increasingly adopting self-help tactics to address cyber intrusions.	Brunoni (2016); Holzer & Lerums (2016); Messerschmidt (2013)
Need for a Legal Framework:	
Territorial sovereignty in cyberspace lacks a legal framework, and poor attribution capabilities perpetuate the issue. Hacking back is limited by legal implications, as it entails intruding on another network to cause significant damage or recover data from the attacker's network and is, therefore, not permitted, given the lack of an immediate threat response.	Balitzer (2015); Lemay & Leblanc (2021); Shires (2020)
Active Cyber Defense:	

Passive defense was deemed insufficient in cyberspace by 2005, as it allowed attackers to operate with minimal perceived risk, creating an imbalance that favored attackers and resulted in double payments for firms, who had to pay for both defensive technologies and the costs of successful attacks.	Christen et al (2020); Craig et al. (2015)
Active defense strategies like hacking back have been advocated for legalization by numerous commentators in corporate cybersecurity.	Balitzer (2015); Cook (2018); Porch (2020)
The tech industry raised concerns about a hacking law similar to the ACDC Act; however, the act could establish a government-private sector partnership that collaborates with CISA's information-sharing provisions to assist organizations in staying ahead of cyber threats.	Porch (2020)
Political Support for Hacking Back:	
The ACDC Act proposed by Republican Tom Graves in 2017 (and reintroduced in 2019) aims to amend the CFAA, permitting individuals and companies to disrupt and identify attacks and retrieve stolen data beyond their networks. Private offensive cyber operations seem increasingly likely, even if the bill is not passed.	Cook (2018); Pattison (2020): Porch (2020)
Despite criticism labeling hack back as the "worst cybersecurity policy idea," policymakers in the US and abroad are advocating for giving companies greater autonomy in defending themselves against cyber attackers.	Shackelford et al. (2019)

Table 4: Trends in Research on Hacking Back

The trends listed in Table 4 indicate the literature from fully reviewed articles. Given the apprehensions of hacking back, the literature specified two groups: those supporting it and individuals with opposing perspectives. Another trending topic is that corporations are already hacking back even though laws prohibit such retaliation. Other trending topics include political support for hacking back, the need for an improved legal framework, and active cyber defense.

CONCLUSION AND FUTURE RESEARCH

This research paper undertook a scoping review that establishes a uniform definition for hacking back, identifies patterns in existing literature, and explores alternatives to hacking back. The study's objectives are reflected in Tables 2-4, which present synthesized analyses. The review indicates that hacking back is a rapidly expanding field with polarizing viewpoints on whether or not to support it. With businesses already engaging in hacking back and increasing cyber-attacks, this topic necessitates further empirical and scholarly investigations. Future research should explore alternative solutions, attribution, developing an appropriate legal framework, and modifying laws to reflect current hacking back practices.

REFERENCES

1. Abbas, A. F., Jusoh, A., Mas, A., Alsharif, A. H., & Ali, J. (2022) Bibliometrix analysis of information sharing in social media, *Cogent Business & Management*, *9*(1), https://doi.org/10.1080/23311975.2021.2016556
2. Abbas, A. F., Jusoh, A., Masod, A., Ali, J., Ahmed, H., & E, A. R. H. (2021), A Bibliometric analysis of publications on social media influencers using vosviewer, *Journal of Theoretical and Applied Information Technology*, *99*(23), 5662–5676.
3. Adam, I., Jusoh, A., & Streimikiene, D. (2019) Scoping research on sustainability performance from manufacturing industry sector, *Problems and Perspectives in Management*, *17*(2). https://doi.org/10.21511/ppm.17(2).2019.10
4. Ali, J., Jusoh, A., & Abbas, A. F. (2021). Thirty- eight years of ' wellbeing ' research: Bibliometric analysis of open access documents, *Studies of Applied Economics*, *October*, 1–11, https://doi.org/10.25115/eea.v39i10.5412
5. Arksey, H., and L. O'Malley. 2005 Scoping studies: Towards a methodological framework, *Int. J. Social Res. Methodol*. 8 (1): 19–32, https://doi.org/10.1080/1364557032000119616
6. Broeders, D. (2021) Private active cyber defense and (international) cyber security—pushing the line? *Journal of Cybersecurity*, *7*(1), tyab010
7. Couzigou, I. (2020) Hacking-back by private companies and the rule of law, *Heidelberg Journal of International Law*.
8. Fisher M. (2013, May) Should the U.S. allow companies to 'hack back' against foreign cyber spies? The Washington Post
9. Guo, J., Yuan, H., Xu, M., & Yang, X. (2022, August) Mimic Honeypot Design and Analysis, In *2022 2nd International Conference on Frontiers of Electronics, Information and Computation Technologies (ICFEICT)* (pp. 604-609). IEEE.
10. Holzer, C. T., & Lerums, J. E. (2016) The ethics of hacking back, In *2016 IEEE Symposium on Technologies for Homeland Security (HST)* (pp. 1-6), IEEE.

11. Kavanaugh, M. S., V. Stamatopoulos, D. Cohen, and L. Zhang. 2016 Unacknowledged caregivers: A scoping review of research on caregiving youth in the United States, *Adolesc. Res. Rev*., 1 (1): 29–49, https://doi.org/10.1007/s40894-015-0015-7.
12. Levac, D., H. Colquhoun, and K. K. O'Brien. 2010. Scoping studies: Advancing the methodology, *Implementation Sci*. 5 (1): 1–9, https://doi.org/10.1186/1748-5908-5-69.
13. Porch, A. M. (2020) Spoiling for a fight: Hacking back with the Active Cyber Defense Certainty Act, *SDL Rev.*, *65*, 467.
14. Rabkin, J., & Rabkin, A. (2016) Hacking back without cracking up, *Aegis Series Paper*, *1601*.
15. Rundle, J. (2021, July 08) Letting businesses 'hack back' against hackers is a terrible idea, cyber veteran says, *Wall Street Journal*, https://www.wsj.com/articles/letting-businesses-hack-back-against-hackers-is-a-terrible-idea-cyber-veterans-say-11625736602
16. Smith, F. A. (2017) Should libraries even consider hacking back if attacked?, *Computers in Libraries*, *37*, 14-16.
17. Thomas, G. (2017, October) On the offensive: Is 'hacking back ethical?, In *Higher Degree by Research Symposium*.